

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently amended) A ~~graphical user interface rendered on computer~~
2 ~~system a display device configured to display a graphical~~ the graphical user
3 interface for configuring a new service ~~detection process~~ alert rule, the graphical
4 user interface comprising:

5 a first field that ~~depicts choices for entities~~ allows a user to specify an
6 entity to track in the network;

7 a second field that allows the user to specify a system to track if the
8 selected entity is providing or consuming a service whether the rule is to be
9 applied when the specified entity is providing or consuming a new service;

10 a third field that ~~depicts a range over which to track an entity selected in~~
11 the first field allows the user to specify a range of network entities to which the
12 new service is unprecedented; and

13 a fourth field that allows the user to specify a severity for an alert
14 generated if a new service is detected.

1 2. (Currently amended) The ~~graphical user interface~~ computer system of
2 claim 1 wherein the fields are linguistically tied together on the interface to form
3 a sentence that corresponds to a rule.

1 3. (Currently amended) The ~~graphical user interface~~ computer system of
2 claim 1 further comprising:

3 a list of new service detection rules stored in the detection system.

1 4. (Currently amended) The ~~graphical user interface~~computer system of
2 claim 1 wherein the first field allows a user to specify the entity to track as “a
3 specific host”, “any host in a specific role”, “any host in a specific segment” or
4 “any host.”

1 5. (Currently amended) The ~~graphical user interface~~computer system of
2 claim 1 wherein the third field specifies details for the extent of the comparison
3 for the entity specified in the first field as “host”, “in its role”, “in its segment” or
4 “anywhere” in the network.

1 6. (Currently amended) The ~~graphical user interface~~computer system of
2 claim 1 wherein event severity is a numerical value entered by the user.

1 7. (Currently amended) The ~~graphical user interface~~computer system of
2 claim 1 wherein the fields are implemented as pull-down fields.

1 8. (Currently amended) A method for detection of a new service involving
2 a host in a network, the method comprises:
3 retrieving a baseline list of port and/or service protocols used by a host
4 being tracked, the baseline list listing service and/or port protocols used by that
5 host over a baseline period that is of a longer duration ~~that~~than a current period;
6 retrieving a current list of service and/or port protocols for the current
7 period used by the host being tracked;
8 determining whether there is a difference in the protocols, by finding a
9 protocol that was in the current list but was not in the baseline list; and if there is
10 a difference;
11 determining whether the host is providing or using the new service;

12 identifying an alert rule corresponding to whether the host is providing or
13 using the new service; and
14 _____ issuing an alert based at least on the identified alert rule and whether the
15 host is providing or using the new service, indicating a new service involving the
16 tracked host.

1 9. (Currently amended) The method of claim 8 further comprising:
2 determining if the host is ~~providing~~ sending traffic using a protocol not in
3 the current list or using the new service ~~receiving traffic with a protocol not in the~~
4 current list.

1 10. (Cancelled)

1 11. (Currently amended) The method of ~~claim 10~~ claim 9 further
2 comprising:
3 retrieving a value corresponding to ~~the alert~~ an alert severity level set for
4 violation of the rule.

1 12. (Previously presented) The method of claim 8 wherein a property of
2 the host being tracked is that the host is at least one of a specific host, any host in
3 a specific role, any host in a specific segment, or any host.

1 13. (Previously presented) The method of claim 8 wherein the extent of
2 the determining is configured for that host, in its role, in its segment or anywhere
3 in the network.

1 14. (Original) The method of claim 8 wherein the baseline and current lists
2 of protocols are provided from data in a connection table.

1 15. (Currently amended) A computer program product residing on a
2 computer readable medium for detection of new services in a network, the
3 computer program product comprising instructions for causing a computer to:
4 retrieve a baseline list of port and/or service protocols used by a host
5 being tracked, the baseline list listing service and/or port protocols used by that
6 host over a baseline period that is of a longer duration than a current period;
7 aggregating communication information between every host pair;
8 retrieve a current list of service and/or port protocols for the current period
9 used by the host being tracked;
10 determine whether there is a difference in the protocols, by identifying a
11 protocol that was in the current list but was not in the baseline list; and if there
12 is a difference;
13 determine whether the host is providing or using the new service;
14 identify an alert rule corresponding to whether the host is providing or
15 using the new service; and
16 issue an alert based at least on the identified alert rule and whether the
17 host is providing or using the new service, indicate a new service involving the
18 tracked host.

1 16. (Currently amended) The computer program product of claim 15
2 further comprising instructions to:
3 determine if the host is ~~providing~~ sending traffic using a protocol not in
4 the current list or ~~using the new service~~ receiving traffic with a protocol not in the
5 current list.

1 17. (Cancelled)

1 18. (Original) The computer program product of claim 15 wherein
2 instructions to indicate further comprise instructions to:

3 issue an alert if the new service is detected.

1 19. (Previously presented) The computer program product of ~~claim 17~~
2 claim 15 further comprising instructions to:
3 retrieve a value corresponding to the alert severity level set for violation of
4 the rule.

1 20. (Previously presented) The computer program product of claim 15
2 wherein a property of the host being track is that the host is at least one of a
3 specific host, any host in a specific role, any host in a specific segment, or any
4 host.

1 21. (Previously presented) The computer program product of claim 15
2 wherein the extent of the determining is configured to for that host, in its role, in
3 its segment or anywhere in the network.

1 22. (Original) The computer program product of claim 15 further
2 comprising instructions to:
3 access a connection table to provide data for the baseline and current lists
4 of protocols.